AMENDMENTS TO THE SPECIFICATION:

Please replace the paragraph on page 1, lines 29-35, with the following paragraph:

At the same time cryptographic algorithms are evolving. This evolution recently took a quantum leap due to the request of the US National Institute of Standards (NIST) for a replacement cipher respectively an advanced encryption standard (AES) for Data Encryption Standard (DES), the most commonly used block cipher. In the near future, embedded cryptographic systems will offer the choice between triple DES (DES run three times) and the winner of the AES competition, which is now known to be Rijndael. The advantage of the former is that it is well tested. The advantage of the latter is that it is faster and more flexible.

Please replace the paragraph from page 6, line 36, through page 7, line 14, with the following paragraph:

Fig. 1 shows a cryptographic system 1 for carrying out cryptographic operations. The system comprises a first cryptographic algorithm means 2, which can be the Rijndael algorithm, for enabling the cryptographic operations. In general, the term cryptographic operation can be understood as a mathematical transformation on the represented form of data as to effect confidentiality, verifiable authenticity, integrity, temporality, non-reputability, et cetera executed in a manner as to resist adversarial alteration. In the embodiment according to Fig. 1 a secret first key is located within the first cryptographic algorithm means 2 and it will be used for ciphering data which is inputted through input line 2a. If the first cryptographic algorithm is not symmetric, then a special protocol or two separate input lines 2a – one for enciphering and one for deciphering – would make sure that the right algorithm is used. The cryptographic system receives input streams from input means 3 and sends output streams by output means 4. The input streams are transformed to output streams by the cryptographic operation. An input stream can be a plaintext or an enciphered text. The corresponding output stream is an enciphered text, respectively a deciphered text.

Please replace the paragraph from page 7, line 16, through page 8, line 1, with the following paragraph:

Receiving means 5 are used to receive a control stream which includes ~~is including~~ at least one apoptosis key K_i. The receiving means 5 and the input means 3 could be the same means, wherein the distinction between an input stream and a control stream would have to be made by a defined protocol. The control stream is supplied to checking means 6. At least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i are preferably located within the checking means 6. If there is only one test plaintext P_i then this test plaintext P_i along with the apoptosis key K_i of a received control stream will be supplied through a further input line 2b to the first cryptographic algorithm means 2. The input of this further input line 2b is enciphered under the first cryptographic algorithm and with the apoptosis key K_i . The resulting enciphered plaintext P_i is supplied to the checking means 6 by an interconnecting means 2c. The checking means 6 performs a step of comparing the resulting enciphered plaintext P_i with the stored test ciphertext C_i . If the comparing shows correspondence then the checking means 6 triggers a switching means 7 to stop the ciphering by the first cryptographic algorithm means 2. A continued cryptographic operation can be enabled by switching to a second cryptographic algorithm means 8, which can be Triple DES or International Data Encryption Algorithm (IDEA), for example. It is also ~~Also~~ possible ~~is~~ to apply a cascaded list of different cryptographic algorithm means and switch them in the defined order. The resulting enciphered plaintext P_i is supplied to the checking means 6 by an interconnecting means 2c. In the embodiment according to Fig. 1, the secret second key is located within the second cryptographic algorithm means 8 and ~~it~~ will be used for ciphering data which is inputted through input line 8a.

Please replace the paragraph at page 15 (the abstract), beginning at line 4, with the following amended paragraph:

An embedded cryptographic system comprises at least one test plaintext/ciphertext pair P_i, C_i for which the key has been destroyed or stored at a very safe place. If at some later date, at least one apoptosis key K_i is presented to the cryptographic system which has the property that C_i

is the enciphered image of P_i under K_i, then the algorithm could be broken and should not be used any more. Instead a more conservative algorithm should be used. The method for changing the ciphering by an embedded cryptographic system includes the step of checking whether at least one test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under an apoptosis key K_i and the step of switching off the used cryptographic mode in case of a positive checking result. ~~In order to enable the step of checking a protocol has to define a control stream with at least one key to be checked. The checking will be done as soon as such as control stream is received by the cryptographic system. The advantage of this solution is the fact, that there is not need for controlling respectively trusting the manufacturer or a security service. The embedded cryptographic system can receive the key or a collection of keys $\{K_i\}$ from anywhere.~~